ROCZNIKI POLSKIEGO TOWARZYSTWA MATEMATYCZNEGO
Seria II: WIADOMOŚCI MATEMATYCZNE VII (1964)

wmptm 1897

Ministerstwo Nauki i Szkolnictwa Wyższego

K. Szymiczek (Katowice)

O równaniu $a^x - b^x = (a-b)c^y$

1. H. J. Kanold ([3], str. 131) udowodnił między innymi następujące twierdzenie (1):

Jeśli p i q są dowolnymi liczbami pierwszymi oraz a i b dowolnymi liczbami naturalnymi, to równanie

$$1+q^a+q^{2a}+\ldots+q^{(p-1)a} = b^p$$

(albo $q^{ap}-1 = (q^a-1)b^p$) nie ma rozwiązań prócz przypadków, gdy $p = q = 2$, $a = b = 3$ oraz $p = 2$, $q = 3$, $a = 1$, $b = 2$.

W przypadku, gdy $a = 1$, twierdzenie to udowodnił także A. Rotkiewicz [5].

Celem tego artykułu jest udowodnienie twierdzenia, że *równanie*

$$a^x - b^x = (a-b)c^y \tag{1}$$

posiada co najwyżej jedno rozwiązanie w liczbach naturalnych x, y, oraz podanie warunków koniecznych pozwalających wyznaczyć ewentualne rozwiązanie równania (1).

Dla $a = 2$, $b = 1$ równanie (1) nie posiada rozwiązań w liczbach naturalnych c, x, y przy $y > 1$. Wiadomo bowiem, że żadna liczba Mersenne'a nie jest potęgą liczby naturalnej o wykładniku większym od jedności. Poza tym przypadkiem równanie (1) posiada rozwiązania w liczbach a, b, c, x, y, przy $y > 1$, np. $3^5-1 = 2\cdot 11^2$, $7^4-1 = 6\cdot 20^2$. Są to więc jedyne rozwiązania równań $3^x-1 = 2\cdot 11^y$, $7^x-1 = 6\cdot 20^y$.

Prawdziwość twierdzenia, że równanie (1) może posiadać co najwyżej jedno rozwiązanie, wynika z twierdzenia Zsigmondy'ego-Birkhoffa-Vandivera (Z-B-V) [1], [4] o istnieniu dzielnika pierwszego pierwotnego liczby $a^x - b^x$. Wynika stąd także pewien warunek konieczny, jaki musi spełniać liczba x w równaniu (1), mianowicie, że o ile rozwiązanie istnieje, to liczba c ma czynnik pierwszy p taki, że $x \mid p-1$.

(1) P. J. McCarthy ([2], str. 46) pisze powołując się na to twierdzenie: „Kanold proved that the Diophantine equation $x^\beta + x^{\beta-1} + \ldots + x + 1 = y^r$ has no solution with x a prime and $r > 1$ except $x = 3$, $\beta = 1$, $y = r = 2$". Jest to oczywiście sformułowanie dalekie od twierdzenia Kanolda; poza tym takie twierdzenie jest fałszywe, jak to wykazują cytowane wyżej przykłady.

Bezpośredni dowód tego twierdzenia wydaje się być interesujący głównie dlatego, że dowód elementarny twierdzenia Z-B-V [4] jest długi i skomplikowany. Ponadto warunki konieczne sformułowane w twierdzeniu z ustępu 3 nie wynikają z twierdzenia Z-B-V.

Jeśli $p^\lambda \mid m$ i $p^{\lambda+1} \nmid m$, piszę $p^\lambda \| m$; $[t_1, \ldots, t_k]$ oznacza najmniejszą wspólną wielokrotność liczb $t_1, \ldots, t_k$.

2. Niech a i b będą liczbami naturalnymi, $a > b$, $(a, b) = 1$, p niech będzie liczbą pierwszą i $p \nmid ab$.

DEFINICJA 1. Liczbę pierwszą nieparzystą p nazywamy *dzielnikiem pierwotnym* liczby $a^\Delta - b^\Delta$, jeśli Δ jest najmniejszą liczbą naturalną taką, że $p \mid a^\Delta - b^\Delta$.

DEFINICJA 2. Liczbę $p = 2$ nazywamy *dzielnikiem pierwotnym* liczby $a-b$, jeśli $4 \mid a-b$, oraz *dzielnikiem pierwotnym* liczby a^2-b^2, jeśli $2 \| a-b$.

Oczywiście Δ istnieje i jeśli p jest nieparzyste, to $1 \leqslant \Delta \leqslant p-1$.

Dowód twierdzenia opiera się na trzech następujących lematach:

LEMAT 1. *Jeśli liczba pierwsza p jest dzielnikiem pierwotnym liczby $a^\Delta - b^\Delta$ i $p^\lambda \| a^\Delta - b^\Delta$, to z tego, że $p^\lambda \mid a^m - b^m$, wynika, że $\Delta \mid m$.*

LEMAT 2. *Jeśli liczba pierwsza p jest dzielnikiem pierwotnym liczby $a^\Delta - b^\Delta$ i $p^\lambda \| a^\Delta - b^\Delta$, to $p^{\lambda+\varepsilon} \| a^{\Delta p^\varepsilon} - b^{\Delta p^\varepsilon}$ dla każdej liczby całkowitej nieujemnej ε.*

LEMAT 3. *Jeśli liczba pierwsza p jest dzielnikiem pierwotnym liczby $a^\Delta - b^\Delta$ i $p^\lambda \| a^\Delta - b^\Delta$, to $p^{\lambda+\varepsilon} \mid a^n - b^n$ wtedy i tylko wtedy, gdy $n = \Delta p^\varepsilon q$, gdzie q jest liczbą naturalną.*

Dowody tych lematów można przeprowadzić metodą indukcyjną, podobnie jak w pracy [1].

3. Udowodnię teraz

TWIERDZENIE. *Jeśli a, b, c są liczbami naturalnymi, $(a, b) = 1$, $a > b \geqslant 1$, to równanie (1) ma co najwyżej jedno rozwiązanie w liczbach naturalnych x, y. Jeśli $c = p_1^{\alpha_1} \ldots p_k^{\alpha_k} p^\alpha$, $k \geqslant 0$, $p_1 < \ldots < p_k < p$, $p > 2$ i liczby pierwsze p_i, p są dzielnikami pierwotnymi liczb $a^{\Delta_i} - b^{\Delta_i}$, $a^\Delta - b^\Delta$, oraz $p_i^{\lambda_i} \| a^{\Delta_i} - b^{\Delta_i}$, $p^\lambda \| a^\Delta - b^\Delta$, to jedyne możliwe rozwiązanie równania (1) otrzymujemy przy $y = \lambda/a$. Ponadto $[\Delta_1, \ldots, \Delta_k, \Delta] \mid x$. Jeśli $p = 2$, to równanie (1) nie ma rozwiązań przy $x > 2$.*

Dowód. Przypuśćmy, że równanie (1) ma rozwiązanie w liczbach x, y i $ay > \lambda$. Mamy też $\alpha_i y \geqslant \lambda_i$, gdyż jeśli $p_i \mid a^x - b^x$, to także $p_i^{\lambda_i} \mid a^x - b^x$. Przypuśćmy więc, że $\alpha_i y = \lambda_i + \varepsilon_i$, $\varepsilon_i \geqslant 0$ oraz $ay = \lambda + \varepsilon$, $\varepsilon > 0$. Ponieważ $p_i^{\lambda_i+\varepsilon_i} \mid a^x - b^x$, $p^{\lambda+\varepsilon} \mid a^x - b^x$, więc na podstawie lematu 3 mamy $\Delta_i p_i^{\varepsilon_i} \mid x$ oraz $\Delta p^\varepsilon \mid x$. Wynika stąd, że $x = [\Delta_1 p_1^{\varepsilon_1}, \ldots, \Delta_k p_k^{\varepsilon_k}, \Delta p^\varepsilon]$.

Przyjmując $n = [\Delta_1 p_1^{\varepsilon_1}, \ldots, \Delta_k p_k^{\varepsilon_k}, \Delta]$ otrzymujemy $x = np^\varepsilon$. Udowodnię, że przy $p > 2$

$$(a-b)c^y < a^x - b^x. \tag{2}$$

Mamy mianowicie

$$p^\varepsilon < a^{n(p^\varepsilon-1)-1} + a^{n(p^\varepsilon-2)-1}b^n + \ldots + a^{n-1}b^{n(p^\varepsilon-2)} + a^{-1}b^{n(p^\varepsilon-1)}, \tag{3}$$

gdyż liczba składników nie mniejszych od jedności jest $p^\varepsilon - 1$ i wobec $a > 1$, $n \geqslant 1$, $p > 2$, $\varepsilon \geqslant 1$ jest $a^{n(p^\varepsilon-1)-1} \geqslant 2$. Stąd mnożąc lewą stronę nierówności (3) przez $a-b$ oraz prawą stronę przez a otrzymujemy

$$(a-b)p^\varepsilon < a^{n(p^\varepsilon-1)} + a^{n(p^\varepsilon-2)}b^n + \ldots + b^{n(p^\varepsilon-1)}. \tag{4}$$

Wobec tego, że $\Delta_i p_i^{\varepsilon_i} \mid n$ oraz $\Delta \mid n$, mamy $p_1^{\lambda_1+\varepsilon_1} \ldots p_k^{\lambda_k+\varepsilon_k} p^\lambda \leqslant a^n - b^n$, co razem z nierównością (4) daje nierówność (2).

Równanie (1) nie może więc posiadać rozwiązań przy y spełniającym nierówność $ay > \lambda$, musi zatem być $ay \leqslant \lambda$, skąd $y = \lambda/a$. Ponieważ $p_i \mid a^x - b^x$, $p \mid a^x - b^x$, więc na podstawie lematu 1 jest $\Delta_i \mid x$, $\Delta \mid x$, skąd otrzymujemy $[\Delta_1, \ldots, \Delta_k, \Delta] \mid x$.

Pozostaje rozpatrzyć przypadek, gdy $p = 2$. Ponieważ p jest największym czynnikiem pierwszym liczby c, więc w tym przypadku $c = 2^\alpha$. Jeśli $a^{x-1} + a^{x-2}b + \ldots + b^{x-1} = 2^y$ i $(a, b) = 1$, to a i b są liczbami nieparzystymi oraz x jest parzyste. Rozpatrujemy więc równanie

$$a^{2x} - b^{2x} = (a-b)2^y. \tag{5}$$

Z równania tego mamy

$$\frac{a^x - b^x}{a-b}(a^x + b^x) = 2^y.$$

Równość ta może zachodzić co najwyżej wtedy, gdy $x = 1$, jeśli bowiem $x > 1$, to wobec tego, że $\left((a^x - b^x)/(a-b), a^x + b^x\right) = 1$ albo 2, $a > b \geqslant 1$, zatem przynajmniej jedna z liczb $(a^x - b^x)/(a-b)$ i $a^x + b^x$ posiada czynnik nieparzysty, co wyklucza możliwość równości (5). Twierdzenie zostało więc udowodnione.

Prace cytowane

[1] G. Birkhoff and H. S. Vandiver, *On the integral divisors of* $a^n - b^n$, Annals of Mathematics, 5 (1904), str. 173-180.

[2] P. J. McCarthy, *Odd perfect numbers*, Scripta Mathematica, 23 (1957), str. 43-47.

[3] H. J. Kanold, *Sätze über Kreisteilungspolynome und ihre Anwendungen auf einige Zahlentheoretische Probleme II*, Journal für Mathematik, 188 (1950), str. 129-146.

[4] A. Rotkiewicz, *Elementarny dowód istnienia dzielnika pierwszego pierwotnego liczby* a^n-b^n, Prace Matematyczne IV (1960), str. 21-28.

[5] A. Rotkiewicz, *O własnościach wyrażenia* $a^n \pm b^n$, Prace Matematyczne VI (1961), str. 1-20.